BY ORDER OF THE COMMANDER

AIR FORCE INSTRUCTION 33-115, VOLUME 1

70TH INTELLIGENCE WING
Supplement 1

9 AUGUST 2002

Communications and Information

NETWORK MANAGEMENT

"HOLDOVER"

"The basic publication has changed; impact on supplemental information is under review by the OPR. Users should follow supplemental information that remains unaffected."

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally.

OPR: 70 IW/SCS (TSgt Albert Augson)

Certified by: 70 IW/SC (Lt Col Robert B. Cabell)
Pages: 14
Distribution: L

AFI 33-115 Volume 1, 2 July 1999, is supplemented as follows. This supplement establishes specific policy and outlines procedures for the 70 IW Workgroup Management Program. This supplement applies to all Workgroup Managers (WMs) assigned to the 70 IW staff, subordinate groups, detachments, and operating locations. It does not apply to Air National Guard or Air Force Reserve members.

6.4.6. The following references from AFI 33-115 V1 are applicable tasks for 70 IW Staff and 694th Intelligence Group WMs based on NSA Groundbreaker contract, WM duties, and local network access procedures.

6.4.6.1. (For 70 IW Staff and 694 IG Workgroup Managers Only) Complies with the policies of this instruction and maintains WM certification.

6.4.6.2. (For 70 IW Staff and 694 IG Workgroup Managers Only) Complies with FSA and NCC policies.

6.4.6.3. (For 70 IW Staff and 694 IG Workgroup Managers Only) Performs the installation of equipment, connection of peripherals, and the installing/deleting of user software.

6.4.6.4. (For 70 IW Staff and 694 IG Workgroup Managers Only) Configures user software, modifies software configuration, and performs basic configuration management functions.

6.4.6.5. (For 70 IW Staff and 694 IG Workgroup Managers Only) Sets up and modifies user introduction menus.

6.4.6.6. (For 70 IW Staff and 694 IG Workgroup Managers Only) Performs bulk-loading/updating database files for resident application programs.

6.4.6.7. (For 70 IW Staff and 694 IG Workgroup Managers Only) Performs database recovery for resident application programs.

6.4.6.8. (For 70 IW Staff and 694 IG Workgroup Managers Only) Provides limited software application assistance for commonly used office automation applications purchased from standard Air Force infrastructure support contracts.

6.4.6.9. (For 70 IW Staff and 694 IG Workgroup Managers Only) Performs e-mail address group maintenance, creating, modifying, and deleting directories, moving files from one media to another, and checking files for corruption.

6.4.6.10. (For 70 IW Staff and 694 IG Workgroup Managers Only) Performs initial system diagnostics and trouble-shooting of systems assigned to them.

6.4.6.16. (For 70 IW Staff and 694 IG Workgroup Managers Only) Coordinates support issues with all agencies (e.g. customers, FSA, NCC, etc.).

6.4.6.17. (For 70 IW Staff and 694 IG Workgroup Managers Only) Notifies the unit ADPE EC of any hardware relocation.

6.4.6.19. (For 70 IW Staff and 694 IG Workgroup Managers Only) Isolates and resolves organization computer problems within own abilities, the FSA, and applicable service contract before seeking assistance from the NCC.

6.4.6.21. (For 70 IW Staff and 694 IG Workgroup Managers Only) Coordinates with the facility manager and the base civil engineer for facility support requirements.

6.4.6.33. (For 70 IW Staff and 694 IG Workgroup Managers Only) Promotes user awareness concerning unauthorized or illegal use of computer hardware and software.

6.4.6.38. (For 70 IW Staff and 694 IG Workgroup Managers Only) Ensures organizations do not use shareware or public domain software until approved for use by the DAA after the CSSO, WM, or FSA ensures it is free of viruses, hidden defects, and obvious copyright infringements.

6.4.6.40. (For 70 IW Staff and 694 IG Workgroup Managers Only) Ensures correct management of records created by or stored on computers by coordinating with the unit records manager. These records include information for official use only or information subject to the Privacy Act of 1974. AFMAN 37-123, *Management of Records* (will convert to AFMAN 33-323), gives details on records management for computers. AFMAN 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-339), tells how to dispose of records.

6.4.6.41. (Added) (All) Implementing Information Operations Condition (INFOCON) procedures.

6.4.6.42. (Added) (All) Implement virus definition update procedures

6.4.6.43. (Added) (All) Implement virus reporting procedures

6.4.6.44. (Added) (All) Promote password education

6.4.6.45. (Added) (All) Creates a WM continuity book

Abbreviations and Acronyms

EC-—Equipment Custodian

FSA—Functional System Administrator

INFOCON—Information Operations Condition

NCC—Network Control Center

DAA-—Direct Approval Authority

CSSO——Computer Systems Support Officer

A4.1. (Added) **Table A4.1.** identifies the breakdown of network elements, tasks performed, and assigns responsibility to 70 IW staff and 694 IG workgroup managers.

Table A4.1. Systems and Networks Support Task Breakdown for 70 IW staff and 694 IG WMs.

Classes of Network Elements	**Tasks**	**Area**
Computer/Workstation Single Client System		
	Select operating area	NSA and 9800 area
	Install equipment	NSA high side 9800 area
	Connect peripherals	NSA high side 9800 area
	System startup	NSA and 9800 area
	Maintain hardware	NSA and 9800 area
	Create, modify, delete directories	9800 area
	Construct file system	9800 area
	Move files from one media to another	NSA and 9800 area
	Review file contents	NSA and 9800 area
	Secure files from erasure	NSA and 9800 area
	Check files for corruption	NSA and 9800 area
	Perform system diagnostics	NSA and 9800 area
	Format, partition, repartition to determine available disk space	9800 area
	Format floppies	NSA and 9800 area
	Make copies of floppies	NSA and 9800 area
	Recover from system crash	9800 area
Client Workstation Resident Application Programs		
	Install and delete user software	NSA and 9800 area
	Provide trouble shooting	NSA and 9800 area
	Install/configure software	NSA and 9800 area
	Email/DMS address groups maintenance	9800 area

Attachment 5

QUALITY ASSURANCE

1. (For 70 IW Staff and 694 IG Workgroup Managers Only) Does the WM comply with systems administrator and NCC policies? **(6.4.6.2.)**

2. (For 70 IW Staff and 694 IG Workgroup Managers Only) Does the WM perform the installation of equipment, connection of peripherals, and the installing/deleting of user software? **(6.4.6.3.)**

3. (For 70 IW Staff and 694 IG Workgroup Managers Only) Does the WM configure user software, modify software configuration, and perform basic configuration management functions? **(6.4.6.4.)**

4. (For 70 IW Staff and 694 IG Workgroup Managers Only) Does the WM set up and modify user introduction menus? **(6.4.6.5.)**

5. (For 70 IW Staff and 694 IG Workgroup Managers Only) Does the WM perform bulk-loading/updating database files for resident application programs? **(6.4.6.6.)**

6. (For 70 IW Staff and 694 IG Workgroup Managers Only) Does the WM perform database recovery for resident application programs? **(6.4.6.7.)**

7. (For 70 IW Staff and 694 IG Workgroup Managers Only) Does the WM provide limited software application assistance for commonly used office automation applications purchased from standard Air Force infrastructure support contracts? **(6.4.6.8.)**

8. (For 70 IW Staff and 694 IG Workgroup Managers Only) Does the WM perform e-mail address group maintenance; create, modify, and delete directories; move files from one media to another; and check files for corruption? **(6.4.6.9.)**

9. (For 70 IW Staff and 694 IG Workgroup Managers Only) Does the WM perform initial system diagnostics and trouble-shooting of systems assigned to them? **(6.4.6.10.)**

15. (For 70 IW Staff and 694 IG Workgroup Managers Only) Does the WM coordinate support issues with all agencies (e.g. customers, SA, NCC, etc.)? **(6.4.6.16.)**

16. (For 70 IW Staff and 694 IG Workgroup Managers Only) Does the WM notify the unit ADPE EC of any hardware relocation? **(6.4.6.17.)**

19. (For 70 IW Staff and 694 IG Workgroup Managers Only) Does the WM isolate and resolve organizational computer problems within their own abilities, the FSA, and applicable service contract before seeking assistance from the NCC? **(6.4.6.19.)**

20. (For 70 IW Staff and 694 IG Workgroup Managers Only) Does the WM inform the accountable ADPE EC of computer equipment problems? **(6.4.6.20.)**

21. (For 70 IW Staff and 694 IG Workgroup Managers Only) Does the WM coordinate with the facility manager and the base civil engineer for facility support requirements? **(6.4.6.21.)**

32. (For 70 IW Staff and 694 IG Workgroup Managers Only) Does the WM promote user awareness concerning unauthorized or illegal use of computer hardware and software? **(6.4.6.33.)**

37. (For 70 IW Staff and 694 IG Workgroup Managers Only) Does the WM ensure organizations do not use shareware or public domain software until the CSO certifies it to be free of viruses, hidden defects, and obvious copyright infringements? **(6.4.6.38.)**

39. (For 70 IW Staff and 694 IG Workgroup Managers Only) Does the WM ensure correct management of records created by or stored on computers by coordinating with the unit records manager? These records include information for official use only or information subject to the Privacy Act of 1974. **(6.4.6.40.)**

40. (Added) (All) Does the WM implement Information Operations Condition (INFOCON) procedures? **(6.4.6.41. (Added))**

41. (Added) (All) Does the WM implement virus definition update procedures? **(6.4.6.42. (Added))**

42. (Added) (All) Does the WM implement virus reporting procedures? **(6.4.6.43. (Added))**

43. (Added) (All) Does the WM promote password education? **(6.4.6.44. (Added))**

44. (Added) (All) Has the WM created a continuity book? **(6.4.6.45. (Added))**

Attachment 7 (Added)

WM PROGRAM IMPLEMENTATION PROCEDURES

A7.1. (Added) (All) All groups will follow specific Air Force, ACC, and 70 IW guidance when implementing the WM program.

A7.2. (Added) (All) Based on NSA Groundbreaker contract, WM duties, and local network access procedures; 373rd IG and 543rd IG are authorized to supplement AFI 33-115V1. As a minimum, 373 IG and 543 IG will supplement:

A7.2.1. (Added) (All) Paragraph **6.4.6.**, listing all applicable task for the group workgroup managers. Groups can add task(s) as needed.

A7.2.2. (Added) (All) Attachment 4, listing Classes of Network Elements and all tasks the WMs will perform. Groups can add task(s) as needed.

A7.2.3. (Added) (All) **Attachment 5**, listing all applicable self-inspection checklist questions. Groups can add questions as needed.

A7.3. (Added) (All) For those units geographically separated from the wing or groups, contact your nearest NCC or 3AXXX Functional Manager for training.

A7.4. (Added) (All) **Training.**

A7.4.1. (Added) (All) Each group will create a unit 3AXXX and Non-3AXXX Workgroup Manager Master Task Training Listing (MTTL).

A7.4.1.1. (Added) (All) As a minimum, the following documents will be used for the 3AXXX MTTL: 3A0X1 CFETP; AF JQS 3A0X1-225D, Position Certification For Workgroup Managers; and ACC JQS Workgroup Managers Position Certification Requirements.

A7.4.1.2. (Added) (All) Use AF Form 797, Job Qualification Standard Continuation/Command JQS to create the unit's Non-3AXXX Workgroup Manager Master Task Training List (MTTL.)

A7.4.2. (Added) (All) Training will be accomplished as a minimum with the use of computer-based training (CBTs) (if applicable) hands-on formal or informal training, and/or video, etc.

A7.4.3. (Added) (All) All groups will create a training database to track all training.

A7.4.4. (Added) (All) All groups will provide monthly training metrics to 70 IW Workgroup Program Manager based on ACC reporting guidance.

A7.4.5. (Added) (All) All 3A0Xs (AB-MSgt) are required to register at the USAF CBT site.

A7.4.6. (Added) (All) Groups will create a mandatory rotational shadow plan that allows at least appointed WMs to work with the help desk.

A7.4.7. (Added) (All) Each group will create a WM Individual Position Training Guide (IPTG) or use ACC IPTG. The IPTG is a document used as a training path for WM training and certification.

A7.4.8. (Added) (All) All 3AX01s (AB-MSgt) will be trained and certified to the WM level as part of upgrade and qualification training.

A7.4.8.1. (Added) (All) All appointed WMs must be trained and certified prior to being responsible for completing workgroup managers' duties.

A7.4.8.2. (Added) (All) For those 3AX01s not appointed as WMs, they are only authorized to perform WM tasks under the supervision of those individuals appointed to a network crew position and certified for the tasks being performed.

A7.4.9. (Added) (All) All appointed WMs will complete annual recertification.

A7.4.10. (Added) (All) Each group will use AFI 33-115 V2 and applicable supplements for the training and certification process.

A7.4.11. (Added) (All) All 3A0X1s (AB-MSgt) are required to have OJT records.

A7.5. (Added) (All) **Appointment.**

A7.5.1. (Added) (All) 70 IW and each group will ensure all applicable offices appoint a primary and alternate Workgroup Manager.

A7.5.1.1. (Added) (All) Where only one 3AXXX is assigned, the 3AXXX will always be the primary workgroup manager.

A7.5.1.2. (Added) (All) Where two or more 3AXXXs are assigned, the 3AXXX will always be the primary and alternate workgroup manager.

A7.5.1.3. (Added) (All) Where no 3AXXX is assigned, any AFSC or occupational series can perform WM duties once trained and certified.

A7.5.1.4. (Added) (All) Appointed WMs are an extension of the NCC or equivalent office and a minimum of 50% of the day is dedicated to WM duties.

A7.5.2. (Added) (All) 70 IW and each group will appoint in writing a workgroup program manager to oversee all policy and guidance for the workgroup management program.

A7.5.3. (Added) (All) Each group will appoint a workgroup trainer and certifier.

A7.6. (Added) (All) **Workgroup Program Manager Responsibilities.**

A7.6.1. (Added) (All) Identify WMs for job rotations (18-24 months) to 3AXXX FM.

A7.6.2. (Added) (All) Will ensure appointed WMs receive training and certification.

A7.6.3. (Added) (All) Will ensure each two-letter staff office (or equivalent) appoints a primary and alternate workgroup manager.

A7.6.4. (Added) (All) Will work with the WM trainer and certifier to ensure WMs are trained and certified.

A7.6.5. (Added) (All) Will ensure the unit's workgroup management program is implemented.

A7.6.6. (Added) (All) Will conduct annual WM SAVs.

A7.6.7. (Added) (All) Will ensure appointed WMs receives annual recertification.

A7.6.8. (Added) (All) Will ensure 3AX01s (AB-MSgt) have OJT records.

A7.6.9. (Added) (All) Will ensure each group provides monthly metrics to 70 IW/SCM.

A7.6.10. (Added) (All) Will ensure each group updates WM INFOCON recall roster and provide to 70 IW/RC.

A7.6.11. (Added) (All) Will work with NCC or equivalent office POC to implement and oversee program.

A7.6.12. (Added) (All) Will oversee the program, providing guidance, training, and advice as needed.

A7.6.13. (Added) (All) Manages all workgroup managers ensuring personnel have received the necessary training (duty, upgrade, and contingency) to accomplish the mission.

A7.6.14. (Added) (All) Develops specific 70 IW guidance.

A7.6.15. (Added) (All) Brief WMs on their responsibilities.

A7.6.16. (Added) (All) Brief leadership and supervisors on WM program and WM responsibilities.

A7.6.17. (Added) (All) Create specific 70 IW registration procedures for the DISA site.

A7.6.18. (Added) (All) Ensure all appointed WMs have registered correctly at DISA based on 70 IW specific guidance.

A7.7. (Added) (All) **Workgroup Trainer and Certifier.**

A7.7.1. (Added) (All) WM trainer and certifier will not be the same individual.

A7.7.2. (Added) (All) WM trainer and certifier must be trained and certified on all applicable tasks prior to providing training and certification.

A7.7.3. (Added) (All) Where WM trainer and certifier are not qualified, as a minimum; use any of the following options:

A7.7.3.1. (Added) (All) Work with the nearest Air Force installation to provide training for the WM trainer and certifier.

A7.7.3.2. (Added) (All) Work with the nearest Air Force installation to provide training for WM trainer, certifier and 3A0X1s (AB-MSgt).

A7.7.3.3. (Added) (All) Request funding from unit to send WM trainer and certifier to civilian equivalent school for training.

A7.7.3.4. (Added) (All) Request funding from unit to send WM trainer, certifier, and appointed WMs to civilian equivalent school for training.

A7.7.4. (Added) (All) Will document the 3AX01s (AB-MSgt) OJT training records after completion of training and certification.

A7.7.5. (Added) (All) Will provide training and certification for 3AX01s (AB-MSgt).

A7.7.6. (Added) (All) Will provide appointed WMs annual recertification.

A7.7.7. (Added) (All) Will follow AFI 33-115 V2 and applicable supplements for the training and certification process.

A7.7.8. (Added) (All) If military, must attend AF trainer and certifier course.

A7.8. (Added) (All) **Commander's and Supervisor's Responsibilities.**

A7.8.1. (Added) (All) Will ensure 3AX01s (AB-MSgt):

A7.8.1.1. (Added) (All) Receives and completes WM training and certification.

A7.8.1.2. (Added) (All) Gets applicable time on the job to complete necessary training.

A7.8.1.3. (Added) (All) Have OJT records.

A7.8.1.4. (Added) (All) Are on schedule based on the training track task and time specified.

A7.8.2. (Added) (All) Will ensure WMs are appointed.

A7.8.3. (Added) (All) Will ensure at least appointed WMs are scheduled to work with help desk during mandatory applicable times.

A7.9. (Added) (All) **Organizational Structure.**

A7.9.1. (Added) (All) WMs will serve as the single focal point for their duty section end users computer problems.

A7.9.2. (Added) (All) When the duty sections primary and alternate WM is unavailable or not trained and certified, the help desk will serve as the single focal point for end users computer problems.

Attachment 8 (Added)

WM INFOCON PROCEDURES

A8.1. (Added) (All) The INFOCON system presents a structured, coordinated approach to defend against and react to adversarial attacks on DOD computer and telecommunication Network and systems, especially critical Command, Control, Communications, Computers and Intelligence (C41) systems. INFOCON levels NORMAL (normal activity), ALPHA (increased risk of attack), BRAVO (specific risk of attack), CHARLIE (limited attack), and DELTA (specific attack on DOD equipment and facilities.)

A8.2. (Added) (All) Each group is required to create a WM INFOCON recall roster. The recall roster will list only the appointed WMs for the group as well as subordinate units. 694 IG recall roster will include 70 IW staff WMs.

A8.2.1. (Added) (All) The recall roster will be kept updated and sent to 70 IW/RC by the 5th of every month.

A8.2.2. (Added) (All) Each Group NCC (or equivalent office) POC will be the groups WM recall POC.

A8.3. (Added) (All) Upon notification, 70 IW/RC will contact each group NCC POC to implement the necessary procedures. 70 IW/RC will provide 70 IW/SCS with a courtesy call.

A8.4. (Added) (All) Upon notification, each Group NCC POC will contact all WMs on the recall roster to implement the necessary procedures. Group NCC POC will provide the WM Program Manager with a courtesy call.

A8.5. (Added) (All) Upon notification, WMs within specified time will implement procedures based on the following INFOCON levels. After implementation, WMs will report completion results back up the chain.

A8.5.1. (Added) (All) **INFOCON NORMAL (Specified Time: 20 min)**

A8.5.1.1. (Added) (All) Identify all mission critical information and information systems (including applications and databases) and their operation importance.

A8.5.1.2. (Added) (All) On a continuing basis, conduct normal practices, to include:

A8.5.1.3. (Added) (All) Conduct education and training for users.

A8.5.1.4. (Added) (All) Ensure through education users have effective passwords in place.

A8.5.1.5. (Added) (All) Be alert for, and report unauthorized network activity to your local Information System Security Officer.

A8.5.1.6. (Added) (All) Ensure normal security systems are operating properly.

A8.5.1.7. (Added) (All) Perform other actions identified by higher authority.

A8.5.2. (Added) (All) **INFOCON ALPHA: (Low Activity) – Increased risk of attack. (Specified Time: 45 min)**

A8.5.2.1. (Added) (All) Advise local SPTS/SC of any unusual activity and begin incident reporting to local SPTS/SC.

A8.5.2.2. (Added) (All) Alert all personnel to be particularly suspicious/inquisitive about any requesting direct access or computer passwords to access 70 IW networks, systems databases and/or other communication mediums.

A8.5.2.3. (Added) (All) Review user policies of computer/network including Internet and electronic mail traffic.

A8.5.2.4. (Added) (All) Ensure CIKs to STU-IIIs and other secure telephone devices are controlled.

A8.5.3. (Added) (All) **INFOCON BRAVO: (Significant Activity) – Specific Risk of Attack. (Specified Time: 75 min)**

A8.5.3.1. (Added) (All) Be placed on standby status for possible recall after normal working hours.

A8.5.3.2. (Added) (All) Notify all base computer users of increased security awareness procedures.

A8.5.3.3. (Added) (All) Verify operational status of all spare equipment.

A8.5.3.4. (Added) (All) Advise users to consider using protected mediums (such as STU-IIIs, secure fax, Secret IP Routed Network [SIPRnet] to conduct official business.)

A8.5.4. (Added) (All) **INFOCON CHARLIE: (Serious Activity) – Limited Attack(s). (Specified Time: 75 min)**

A8.5.4.1. (Added) (All) Assess and report the damage to SCB.

A8.5.4.2. (Added) (All) Identify and respond to the threat or problem.

A8.5.4.3. (Added) (All) Increase protection of external communication closets power supplies.

A8.5.4.4. (Added) (All) Expect disconnection of all critical C4I command and control systems and/or databases capable of operating in the stand-alone mode.

A8.5.5. (Added) (All) **INFOCON DELTA: (Critical Activity) – General Attack(s). (Specified Time: 30 min)**

A8.5.5.1. (Added) (All) Implement emergency restoral procedures for affected critical mission systems.

A8.5.5.2. (Added) (All) Expect disconnection of all C4I critical systems and/or databases capable of operating in the stand-alone mode.

A8.5.5.3. (Added) (All) Expect disconnection of non-mission critical systems.

A8.5.5.4. (Added) (All) Expect isolation of compromised systems from the rest of the network.

A8.5.5.5. (Added) (All) Expect the move of critical mission application to virtual private network connections on SIPRnet.

A8.5.5.6. (Added) (All) Ensure increased reporting requirements identified by higher authorities are met.

Attachment 9 (Added)

VIRUS DEFINITION UPDATE PROCEDURES

A9.1. (Added) (All) At a minimum, virus definitions for NSAnet, SIPRnet, and NIPRnet must be checked at least 3 times a week to ensure they are current. Workgroup Managers will:

A9.1.1. (Added) (All) Ensure network and stand-alone computers must have the most current definitions.

A9.1.2. (Added) (All) Ensure a scan is done after each new virus definition file is downloaded.

A9.1.3. (Added) (All) Ensure only authorized virus scan software is loaded on computers.

Attachment 10 (Added)

VIRUS REPORTING PROCEDURES

A10.1. (Added) (All) Anyone discovering a virus will notify the WM responsible for the system or media. The WM will report up the chain to the ISSM. Workgroup Managers will also:

A10.1.1. (Added) (All) Isolate the AIS(s) by disconnecting the LAN cable from any network or by preventing any file transfers.

A10.1.2. (Added) (All) Scan the affected AIS(s) and removable magnetic media in the immediate area.

A10.1.3. (Added) (All) Await final instructions for cleanup from Chief Information Officer.

A10.1.4. (Added) (All) File an Incident Report as outlined in Joint DODIIS/Cryptologic SCI Information System Security Standards, chapter 7, paragraph 3.4 if a virus is found.

Attachment 11 (Added)

PASSWORD EDUCATION

A11.1. (Added) (All) Workgroup Managers will ensure users are aware:

A11.1.1. (Added) (All) Password is not the same as the users surname.

A11.1.2. (Added) (All) Password is not a name, birth date, phone number, SSN, etc.

A11.1.3. (Added) (All) Password is not a word in the English or foreign language dictionary.

A11.1.4. (Added) (All) Password is not a string of the same letter.

A11.1.5. (Added) (All) Password is not any of the above with a single digit appended or prepended.

A11.1.6. (Added) (All) To use upper and lowercase, digits, punctuation, and special characters when allowed.

A11.1.7. (Added) (All) To use a combination of two or more short words.

A11.1.8. (Added) (All) To use acronyms that are meaningful only to the users.

JAMES O. POSS, Colonel, USAF
Commander